

ABSTRACT OF THE DISCLOSURE

A computer system for detecting and monitoring network intrusion events from log data received from network service devices in a computer network, the computer system having discrete modules associated with a function performed on the log data received, the computer system having an event parser in communication with at least one network service device, the event parser being able to receive log data in real time from the device, the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the information to create a corresponding event object concerning the intrusion event. The compute system also includes an event manager in communication with the event parser, the event parser being able to receive the event object, the event manager being configured to evaluate the event object according to at least one predetermined threshold condition such that, when the event object satisfies the predetermined threshold condition, the event manager designates the event object to be broadcast in real time, and an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event object in real time as an intrusion alarm. The computer system may use a graphical user interface in communication with the event broadcaster, the graphical user interface having a display screen for displaying an intrusion alarm and the information contained within the corresponding event object received from the event broadcaster. The graphical user interface may be configured to allow a user to initiate queries and communicates with a report servlet coupled to the graphical user interface, the report servlet recalling stored event objects in response to user queries from the graphical user interface and displaying recalled event objects

[illegible]